Reg. No.												

Question Paper Code	11571

M.E. - DEGREE EXAMINATIONS, NOV/DEC 2022

Second Semester

M.E. - Embedded Systems Technologies

20PESEL207 - CRYPTOGRAPHY AND NETWORK SECURITY

(Regulations 2020)

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks, K-Level,CO
1.	How many keys are required for two people to communicate via a cipher?	2,K1,CO1
2.	What is the difference between SubBytes and SubWord?	2,K1,CO1
3.	What requirements must a public key cryptosystems fulfill to be a secure algorithm?	2,K1,CO2
4.	What characteristics are needed in a secure hash function?	2,K1,CO2
5.	How IPSec does offer the authentication and confidentiality services?	2,K1,CO3
6.	What is the role of Ticket Granting Server in inter realm operations of Kerberos?	2,K1,CO3
7.	Why the leading two octets of message digest are stored in PGP message along with encrypted message digest?	2,K1,CO4
8.	What is IP address spoofing?	2,K1,CO4
9.	What are the benefits of packet sniffing?	2,K1,CO5
10.	Why are wireless networks vulnerable to DoS attacks?	2,K1,CO5

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	(i) Draw the general structure of Advanced Encryption Standard and explain the encryption decryption process.	10,K2,CO1
		(ii) Mention the strengths and weakness of Advanced Encryption Standard algorithm.	3,K2,CO1
		OR	
	b)	Compute the output of the MixColumns transformation for the following sequence of input bytes "67 89 AB CD". Apply the InvMixColumns transformation to the obtained result to verify your calculations. Change the first byte of the input from '67' to '77', perform the MixColumns transformation again for the new input, and determine how many bits have changed in the output.	13,K3,CO1
12.	a)	(i) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.	9,K3,CO2
		(ii) Identify the possible threats for RSA algorithm and list their counter measures.	4,K2,CO2

OR

b) Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71and a primitive root α=7. *13,K3,CO2*
(i) If user A has private key X_A=5, what is A's public key Y_A?
(ii) If user B has private key X_B=12, what is B's public key Y_B?
(iii) What is the shared secret key?

13. a) How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. *13,K4,CO3*

OR

b) (i) What is Kerberos? Explain how it provides authenticated service. *6,K2,CO3*
(ii) Explain the format of the X.509 certificate. *7,K2,CO3*

14. a) Define intrusion detection and explain the different types of detection mechanisms, in detail. *13,K2,CO4*

OR

b) (i) Explain firewalls and how they prevent intrusions. *6,K2,CO4*
(ii) What are the positive and negative effects of firewall? *7,K3,CO4*

15. a) Explain in detail about any three types of Attacks That Target Wireless Networks. *13,K3,CO5*

OR

b) Explain in detail about the best method of Authentication *13,K2,CO5*

PART - C (1 × 15 = 15 Marks)

16. a) Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101}: *15,K3,CO6*
a. Show the original contents of State, displayed as a 4 × 4 matrix.
b. Show the value of State after initial AddRoundKey.
c. Show the value of State after SubBytes.
d. Show the value of State after ShiftRows.
e. Show the value of State after MixColumns.

OR

b) Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer. *15,K3,CO6*

Transfer amount	Cryptography functions required
1 – 2000	Message digest
2001 – 5000	Digital signature
5000 and above	Digital signature and encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations.